



# 中华人民共和国通信行业标准

YD/T 2692-2014

---

## 电信和互联网用户个人电子信息保护 通用技术要求和管理要求

General technology and management protection requirements  
for telecom and internet users personal electronic information

2014-10-14 发布

2014-10-14 实施

---

中华人民共和国工业和信息化部 发布

# 目 次

前 言	II
1 范围	1
2 术语和定义	1
3 概述	1
3.1 安全防护范围	1
3.2 安全防护内容	2
4 安全防护要求	2
4.1 收集环节	2
4.2 存储环节	3
4.3 操作环节	3
4.4 转移环节	5
4.5 删除环节	6
参考文献	7

## 前 言

本标准是“电信网和互联网安全防护体系”系列标准之一，该系列标准的结构及名称预计如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》
33. 《域名系统安全防护要求》
34. 《域名系统安全防护检测要求》

35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网应用安全防护要求》
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 WEB应用系统》
61. 《电信和互联网用户个人电子信息保护通用技术要求和管埋要求》（本标准）
62. 《电信和互联网用户个人电子信息保护检测要求》

本标准与YD/T 2693-2013《电信和互联网用户个人电子信息保护检测要求》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国互联网络信息中心、北京和升达信息安全技术有限公司、北京新浪互联信息服务有限公司、深圳腾讯计算机系统有限公司、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司。

本标准主要起草人：封莎、王昕、龚双瑾、魏薇、徐颖、周景泉、许章毅、左洪涛、杨晓光、邱勤、杨淑敏。



# 电信和互联网用户个人电子信息保护通用技术要求和管理要求

## 1 范围

本标准主要规范电信和互联网用户个人电子信息分类别的技术和管理方面的安全防护要求。

本标准主要适用于电信和互联网存储和处理用户个人电子信息的相关系统。

## 2 术语和定义

下列术语和定义适用于本文件。

### 2.1

**电信和互联网用户个人电子信息** Telecom and Internet Users Personal Electronic Information

电信业务经营者和互联网信息服务提供者在提供服务的过程中以电子形式存储和使用的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点、通信内容等信息。

### 2.2

**身份信息** Identity Information

电信和互联网用户个人电子信息的一种，指能够单独或相互结合识别特定用户身份的信息。

### 2.3

**鉴权信息** Authentication Information

电信和互联网用户个人电子信息的一种，指用于鉴定用户身份是否合法的信息。

### 2.4

**日志信息** Log Information

电信和互联网用户个人电子信息的一种，指用户使用电信业务过程中产生的信息。

### 2.5

**内容信息** Contents Information

电信和互联网用户个人电子信息的一种，指用户使用电信业务过程中所传递的信息内容。

### 2.6

**销毁** Destruction

通过消磁、粉碎等技术手段使电子信息载体中存储的信息不可再用，且不可恢复的过程。

## 3 概述

### 3.1 安全防护范围

电信和互联网用户个人电子信息是指电信业务经营者和互联网信息服务提供者在提供服务的过程中以电子形式存储和使用的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点、通信内容等信息。

电信和互联网用户个人电子信息按照内容可以分为身份信息、鉴权信息、日志信息和内容信息，具体如下：

1. 身份信息：指能够单独或相互结合识别特定用户身份的信息，如用户基本资料、通讯录信息和虚拟身份信息。个人用户基本资料包括个人姓名、出生日期、个人有效证件类别和号码、职业、单位、居住地址、家庭成员信息和通信联系方式等；单位用户基本资料包括单位名称、单位有效证件类别和号码、办公或注册地址、通信联系方式、单位负责人和联系人基本信息等。通讯录信息包括存储于用户终端设备或同步到服务器上的联系人列表、电话号码簿等。虚拟身份信息包括用户昵称、级别和积分等。

2. 鉴权信息：指用于鉴定用户身份是否合法的信息，如用户登录各种业务系统的账号和密码、服务密码等。

3. 日志信息：指用户使用电信业务过程中产生的信息，如用户消费信息、服务订购关系、终端信息、访问信息（如 IP 地址）、位置信息、使用服务的时间及使用相关业务的记录（如通话详单、网页购物记录、搜索内容等）。

4. 内容信息：指用户使用电信业务过程中所传递的信息内容，如短信内容记录、移动上网内容及记录、应用平台上交互的信息内容等。

### 3.2 安全防护内容

电信和互联网用户个人电子信息的生命周期可分为收集、存储、操作、转移、删除五个环节。对电信和互联网用户个人电子信息的安全防护要求贯穿于五个环节中：

1. 收集环节：指对电信和互联网用户个人电子信息进行获取并记录的过程。

2. 存储环节：指电信和互联网用户个人电子信息在通信网络单元中存储的过程。

3. 操作环节：指电信和互联网用户个人电子信息收集者操作使用信息的过程。

4. 转移环节：指电信和互联网用户个人电子信息从收集者向第三者的流转过程，包括向公众或特定对象公开、合作伙伴间信息共享、委托加工等情形。

5. 删除环节：指使电信和互联网用户个人电子信息在信息系统中不再可用的过程。

## 4 安全防护要求

### 4.1 收集环节

#### 4.1.1 管理要求

a) 收集用户个人电子信息应当有正当、明确的目的。

b) 收集用户个人电子信息时，应满足以下条件之一。

1) 法律法规明确授权或经用户同意；

2) 与用户有合法的合同关系；

3) 用户自行公开或已合法公开的信息。

c) 收集用户个人电子信息前应采用用户能够知悉的方式，至少向用户明确告知如下事项。

1) 收集用户个人电子信息的目的、方式、类别和留存时限；

2) 用户个人电子信息的使用范围，包括披露或向其他组织和机构提供其用户个人电子信息的范围；

3) 用户个人电子信息的保护措施；

4) 提供用户个人电子信息后可能存在的风险；

5) 不提供用户个人电子信息可能出现的后果；

6) 用户个人电子信息管理者的名称、地址、联系方式等信息；

7) 用户的投诉渠道。

d) 应只收集能够达到已告知目的的最少信息，不得收集与其所告知的收集目的无直接关系的用户个人电子信息。

e) 应采用已告知的手段和方式直接向用户收集用户个人电子信息，不采取隐蔽手段或以间接方式收集用户个人电子信息。

#### 4.1.2 技术要求

a) 通过在线方式进行用户身份信息收集时，应使用加密传输以保障用户在线提交信息的安全性。

b) 应对用户设置访问控制，每个用户只能访问自己所上传的用户信息。

c) 用户鉴权信息应有位数要求，并有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符四种字符中至少三种的组合，且与用户名无相关性）。

d) 应对收集用户个人电子信息的操作进行日志记录，并对日志记录中的身份信息和鉴权信息进行模糊化处理。

e) 身份信息、鉴权信息在用户端显示时应进行模糊化处理，如用户注册页面身份证号码显示、密码找回页面手机号码显示、密码找回页面邮箱显示、用户输入密码显示等。

### 4.2 存储环节

#### 4.2.1 管理要求

a) 对于存储用户个人电子信息的存储介质（如磁阵、硬盘和磁带等）的维护、更换、升级和销毁等操作和管理流程，应制定严格的登记和审批制度并落实。

b) 应采取有效的管理手段加强对涉及用户个人电子信息的系统使用移动存储介质的管控，对向移动介质输出用户个人电子信息的情况进行日志记录，并定期审核。

#### 4.2.2 技术要求

a) 应采取技术手段保障用户个人电子信息的安全性和完整性，鉴权信息应加密存储。

b) 作为后台的存储系统须与前端的用户信息收集系统在物理上进行分离，不得共用服务器。

c) 应实现网络安全域划分，不同安全域之间使用防火墙进行隔离和访问控制。存储系统应处于内部安全域，不对互联网提供服务，并与用户信息收集系统处于不同安全域。

d) 防火墙对存储系统的访问策略应设置为默认拒绝，只对特定的用户信息收集系统、用户信息使用系统及管理终端开放访问权限。

e) 用户个人电子信息必须存储在境内。

### 4.3 操作环节

#### 4.3.1 管理要求

##### 4.3.1.1 业务人员要求

a) 对业务人员操作用户个人电子信息的行为，应建立明确的操作审批流程，定期进行严密的事后审核。

b) 涉及身份信息的操作，业务人员应获得用户的同意，并且按照正常的鉴权流程通过身份认证。

c) 涉及内容信息的查询，业务人员只能在响应用户请求时，并且用户自身按照正常流程通过身份鉴权的情况下，协助用户查询，禁止业务人员擅自进行查询。

##### 4.3.1.2 运维支撑人员要求



a) 对运维支撑人员操作用户个人电子信息的行为，应建立明确的操作审批流程，定期进行严密的事后审核。

b) 运维支撑人员因业务投诉、统计取数、批量业务操作、批量数据修复等原因进行的用户个人电子信息查询、变更必须提交操作申请，按照要求进行操作，不得扩大操作范围。

c) 运维支撑人员因应用优化、业务验证测试等原因需要查询、修改用户个人电子信息时，应使用测试号码进行各项测试。

d) 运维支撑人员因系统维护进行用户个人电子信息的数据迁移（数据导入、导出、备份）必须提交操作申请，并经过审批。

e) 运维支撑人员不应向开发测试环境导出用户个人电子信息，如需导出必须经过申请审批，并进行模糊化处理。

#### 4.3.1.3 开发人员要求

a) 开发人员的工作区域应与生产、内部办公、维护区域分离，并采用严格的访问控制策略和管控手段。

b) 开发人员使用的测试数据不应当包含真实的用户个人电子信息，必须是经过模糊化处理的数据。

c) 开发人员进入可能接触到用户个人电子信息的生产或维护区域时，应有相应的审批制度。

d) 开发人员转岗或离岗前，应完成开发人员的账号回收、审核、网络调整等工作。

#### 4.3.2 技术要求

##### 4.3.2.1 信息系统要求

a) 涉及用户个人电子信息的系统应位于核心安全域，安全域边界采用防火墙、入侵检测系统等防护手段。

b) 应严格管理和限制涉及用户个人电子信息的系统与其他系统的互联互通。

c) 安全边界的网络设备、安全设备应定期进行安全评估和审核，及时修补漏洞，杜绝弱口令。

d) 在系统建设的各个阶段加强用户个人电子信息安全性：

1) 系统在设计阶段，应当根据接口和流程涉及到用户个人电子信息的类型和操作类型（查询、修改、增删），来定义安全需求；

2) 在系统交付阶段分别对系统的接口与流程的安全性进行评估，未达到安全要求的系统原则上不允许上线；

3) 做好上线前的安全评估、基线审核，封堵和修补系统、数据库、中间件、应用层的漏洞，升级安全补丁，防止系统被攻击和入侵。

e) 应定期（至少每月1次）进行系统级和代码级的漏洞扫描（重大变更与系统升级后也需进行），以及时发现所使用的操作系统、中间件、数据库以及程序本身的高危险安全漏洞，及时修补发现的安全漏洞以及配置不符合项。

f) 严格限制可访问和操作用户个人电子信息的人员和账户，遵循权限最小化原则，从技术上限制非授权用户接触用户个人电子信息和合法用户能访问敏感信息的权限。

g) 应设置账号/口令的访问控制，口令长度不少于8位，并有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符四种字符中至少三种的组合，且与用户名或ID无相关性）。

h) 系统账号口令输入尝试次数应做限制，防止口令的暴力破解。



i) 对于无法进行定期修改口令的账号，如内置账号、程序账号等，应在系统升级或重启时落实口令修改工作。

j) 如发生口令遗忘的情况，账号使用人应提出口令重置申请，由系统管理员进行密码重置，重置完毕后，使用者应马上更改重置后的密码。

k) 当程序内的账号密码需要保存在配置文件里时，应只使用适当权限的账号，采用经过验证的算法对账号口令进行加密，并做好账号口令和加密密钥的保护工作。

l) 应记录所有对用户个人电子信息的访问操作，形成日志，记录内容必须至少包括访问人员、访问对象、访问时间、访问操作。

m) 应定期（至少每月）对涉及用户个人电子信息访问和操作的日志进行审计，审计时应特别关注批量访问，保证每次批量访问均为正常业务操作。

#### 4.3.2.2 操作维护终端要求

a) 针对能处理用户个人电子信息的操作维护终端，应制定严格的的安全管理制度。

b) 操作维护终端应统一安装防病毒软件，限制移动存储介质的使用，限制无线网络的使用。

c) 操作维护终端应有统一的接入控制，执行统一的安全策略。

d) 操作维护终端应定期（至少每月1次）进行漏洞扫描，及时进行安全加固。

#### 4.3.2.3 监测能力要求

a) 应对系统中防火墙、入侵检测系统等防护手段的工作状态进行监测，发现异常情况时提供告警，并进行相应处置。

b) 应对涉及用户信息的访问和操作进行监测和日志记录，保留一定期限（至少90天），并定期进行审核，并能对异常操作（如大批量操作等）进行告警。

### 4.4 转移环节

#### 4.4.1 管理要求

a) 不应违背收集阶段告知的使用目的，或超出告知的使用范围转移用户个人电子信息。

b) 不应向其他机构转移鉴权信息和内容信息，如需转移身份信息和日志信息要向用户明确告知包括但不限于以下信息：转移或委托的目的、转移或委托用户个人电子信息的具体内容和使用范围等，并获得用户的明示同意。

c) 向其他机构转移用户个人电子信息时，应保证接收者是达到本标准要求的、合格的接收者，应保障用户个人电子信息在转移过程中的安全，并且应当通过合同明确用户个人电子信息接收者对用户个人电子信息的安全保密责任。

d) 未经用户的明示同意，或法律法规没有明确规定，或未经主管部门同意，不得将用户个人电子信息转移给境外用户个人电子信息获得者，包括位于境外的个人或境外注册的组织和机构。

e) 如需将用户个人电子信息传递至境外，应当符合法律法规的规定，并在以下情形根据主管部门的要求暂停或终止传输。

1) 涉及国家重大利益；

2) 国际条约或协定有特别规定；

3) 接收国对数据没有完善的保护制度，有损当事人权益。

f) 将数据转移至境外，应当订立符合主管部门规定的标准合同，明确以下事项。

1) 存储数据的服务器的存放地点;

2) 明确数据接收者应当遵守的数据安全保密措施;

3) 明确当接收者所在国或者服务器存放地所在国以及其他相关国家通过司法途径要求公开服务器中存储的数据时所应遵循的司法程序。

#### 4.4.2 技术要求

a) 应有完善的数据传输保护机制,包括数据加密、完整性校验等手段。对于跨越互联网或不同等级安全域之间的数据传输,必须进行加密,以实现数据传输的安全。

b) 应对用户个人电子信息的转移操作进行日志记录,并对日志记录中的用户个人电子信息进行模糊化处理。

### 4.5 删除环节

#### 4.5.1 管理要求

a) 涉及用户个人电子信息的业务系统下线时,应删除用户个人电子信息。

b) 在用户个人电子信息使用目的达到后,应立即删除用户个人电子信息或消除其中能够识别具体个人的内容。

c) 超出收集阶段告知的用户个人电子信息留存期限时,应立即删除相关信息。

d) 应具备用户注销身份信息(如用户账户等)的功能,应允许用户删除所提供的用户个人电子信息(如通信地址,绑定的手机号码等)。

#### 4.5.2 技术要求

a) 对于要离开系统的电子信息存储介质,必须采用有效的手段由内部专人负责彻底删除用户个人电子信息后,才可离开其所在的安全区域。

b) 电子信息存储介质如不再使用,应通过消磁、粉碎等技术手段由内部专人负责及时销毁。需要销毁的电子信息存储介质类型包括:硬盘、软盘、光盘、U盘以及各种存储芯片等。

c) 删除用户个人电子信息和销毁电子信息存储介质时,应采用可靠的技术手段保证存储的用户个人电子信息不被还原。

d) 删除用户个人电子信息和销毁电子信息存储介质过程应进行日志记录,包括执行时间、参与人员、处理方式等。

## 参 考 文 献

- [1] 全国人民代表大会常务委员会关于加强网络信息保护的決定，2012
  - [2] 电信和互联网用户个人信息保护規定（中华人民共和国工业和信息化部令第24号），2013
  - [3] GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
-